

Method and system for managing a distributed trust path locally for public key certificates
relating to the trust path of an X.509 attribute certificate

1/7

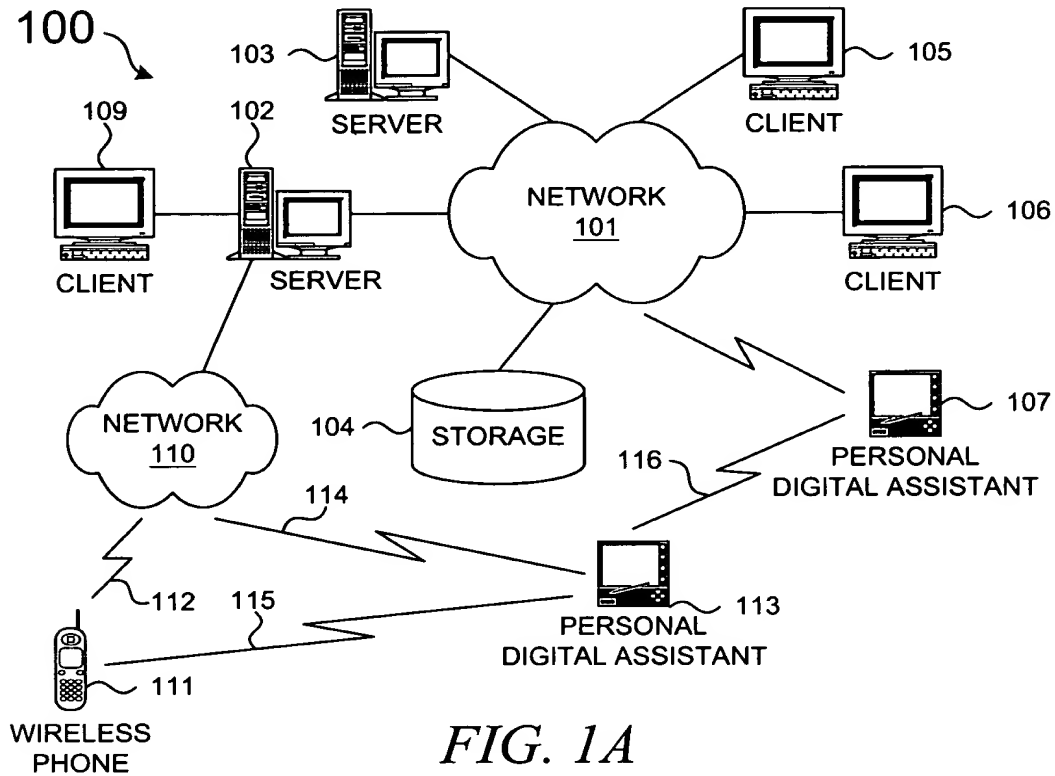


FIG. 1A
(PRIOR ART)

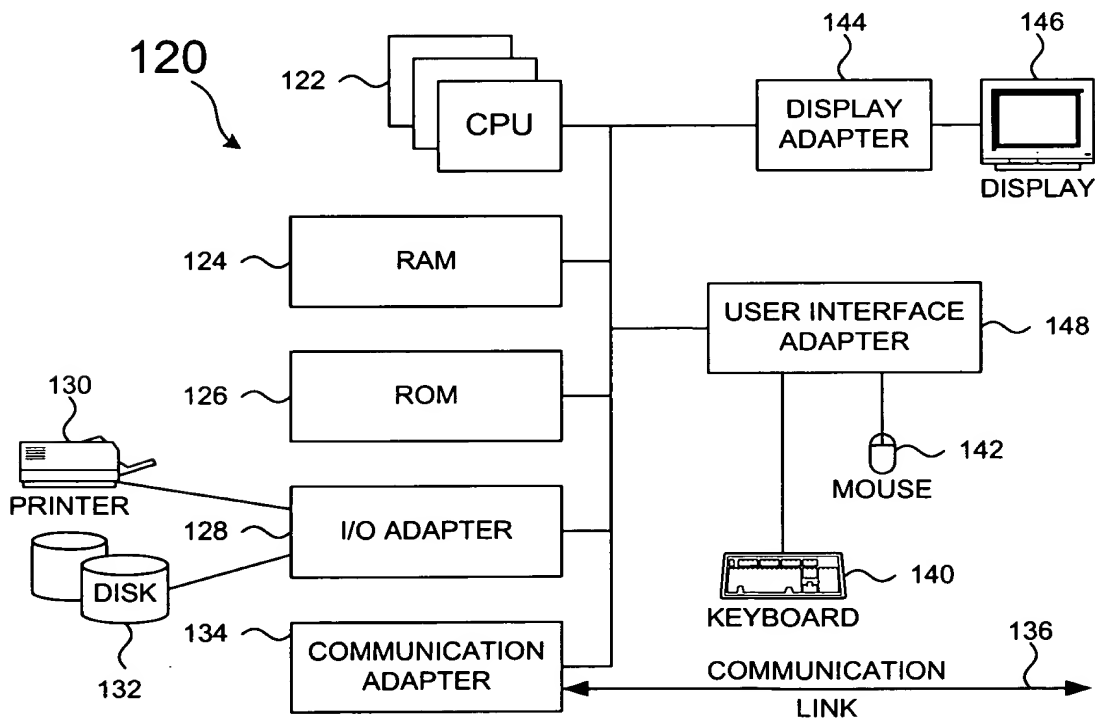


FIG. 1B
(PRIOR ART)

FIG. 1A (PRIOR ART)

Method and system for managing a distributed trust path locator for public key certificates
relating to the trust path of an X.509 attribute certificate

2/7

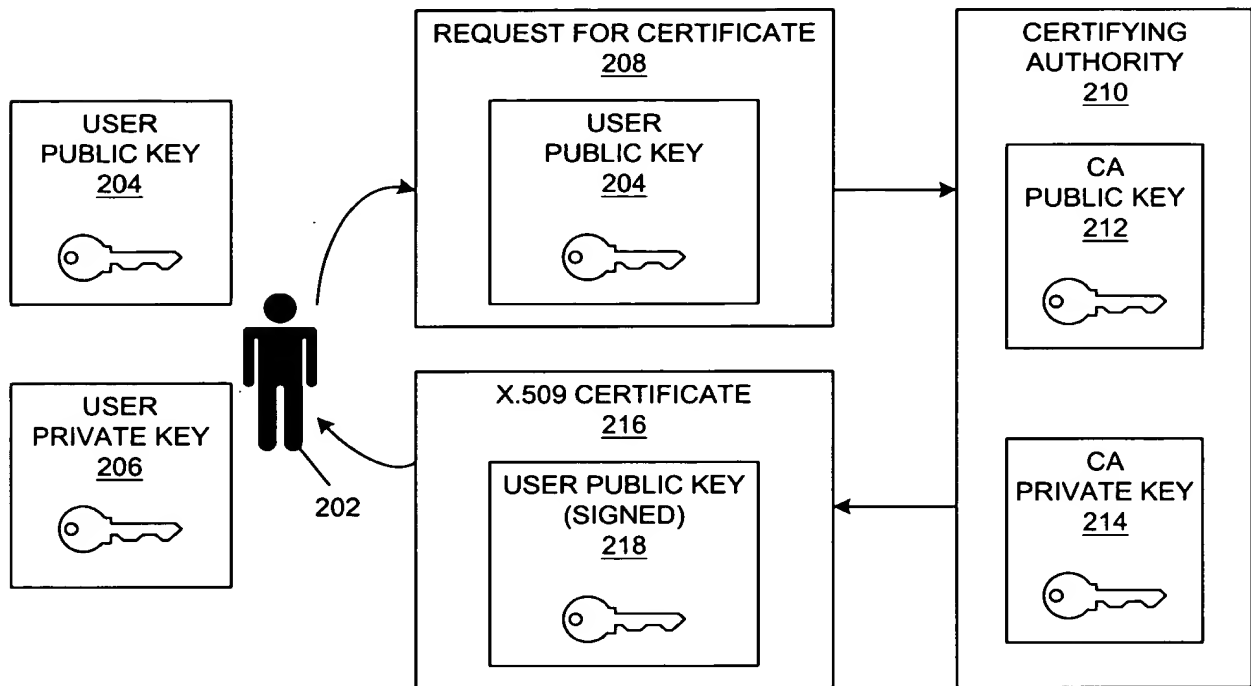


FIG. 2
(PRIOR ART)

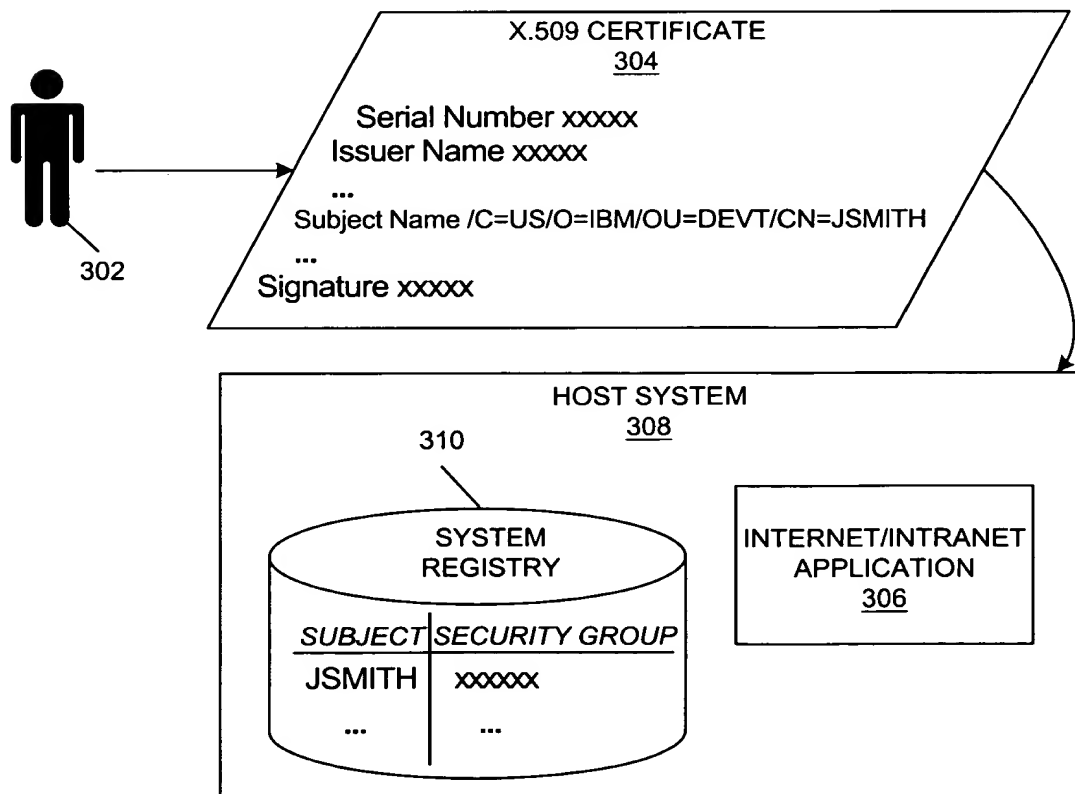
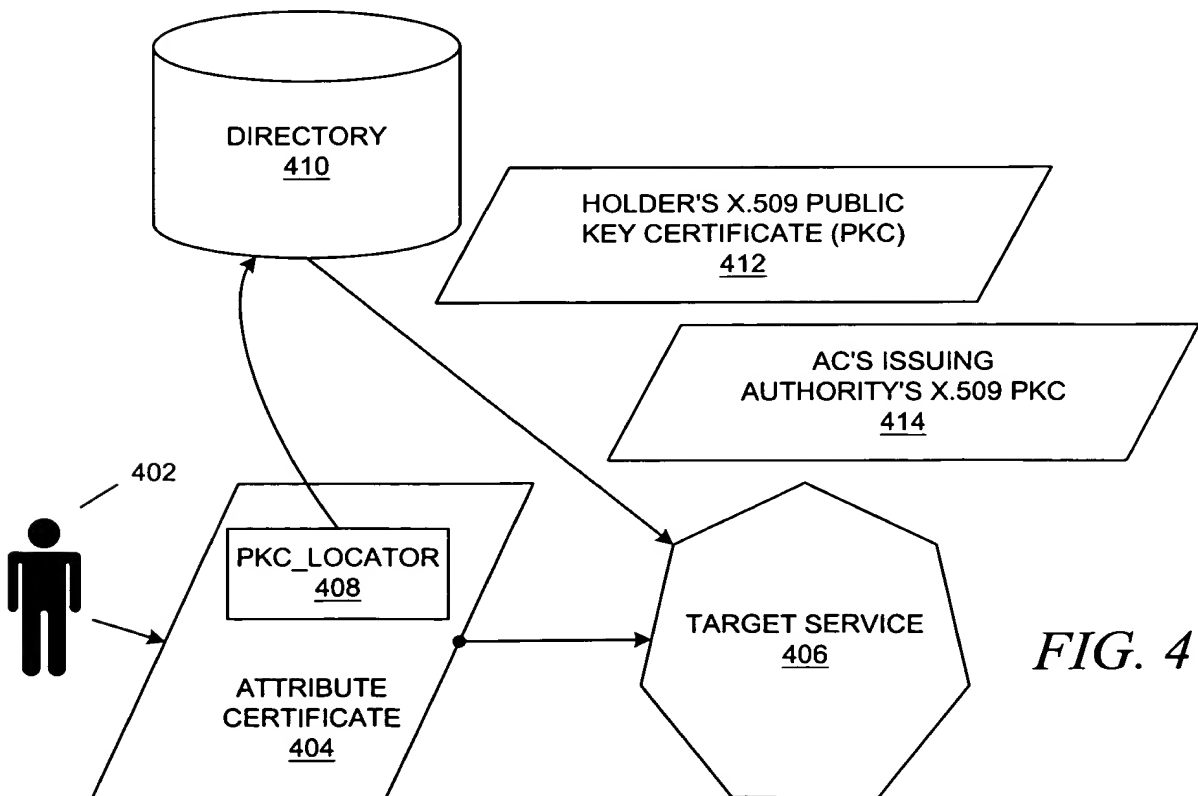
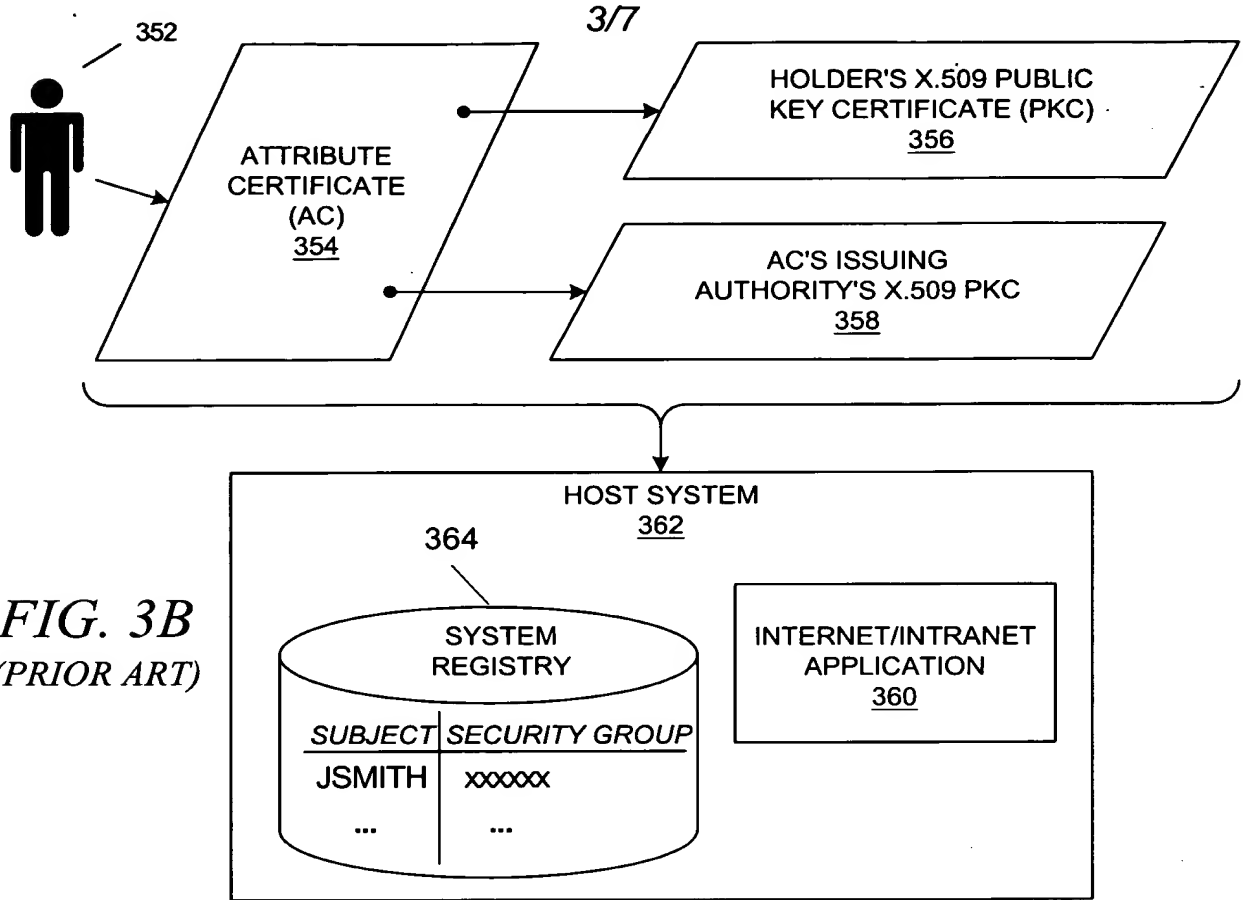


FIG. 3A
(PRIOR ART)

Method and system for managing a distributed trust path locator for public key certificates relating to the trust path of an X.509 attribute certificate



Method and system for managing a distributed trust path look for for public key certificates
relating to the trust path of an X.509 attribute certificate

4/7

Certificate ::= SEQUENCE {
 tbsCertificate TBSertificate,
 signatureAlgorithm AlgorithmIdentifier,
 signature BIT STRING }

TBSertificate ::= SEQUENCE {
 version [0] Version DEFAULT v1,
 serialNumber CertificateSerialNumber,
 signature AlgorithmIdentifier,
 issuer Name,
 validity Validity,
 subject Name,
 subjectPublicKeyInfo SubjectPublicKeyInfo,
 issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,
 subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,
 extensions [3] Extensions OPTIONAL }

Version ::= INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
 notBefore Time,
 notAfter Time }

Time ::= CHOICE {
 utcTime UTCTime,
 generalTime GeneralizedTime }

UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo ::= SEQUENCE {
 algorithm AlgorithmIdentifier,
 subjectPublicKey BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
 extnID OBJECT IDENTIFIER,
 critical BOOLEAN DEFAULT FALSE,
 extnValue OCTET STRING }

FIG. 5A
(PRIOR ART)

09734810-051004

Method and system for managing a distributed trust path for public key certificates
relating to the trust path of an X.509 attribute certificate

5/7

```

AttributeCertificate ::= SEQUENCE {
    acinfo          AttributeCertificateInfo,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue   BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
    version          AttCertVersion DEFAULT v1,
    holder           Holder,
    issuer           AttCertIssuer,
    signature        AlgorithmIdentifier,
    serialNumber     CertificateSerialNumber,
    attrCertValidityPeriod AttCertValidityPeriod,
    attributes       SEQUENCE OF Attribute,
    issuerUniqueID   UniqueIdentifier OPTIONAL,
    extensions       Extensions OPTIONAL
}

AttCertVersion ::= INTEGER { v1(0), v2(1) }

Holder ::= SEQUENCE {
    baseCertificateID [0] IssuerSerial OPTIONAL,
    -- the issuer and serial number of
    -- the holder's Public Key Certificate
    entityName        [1] GeneralNames OPTIONAL,
    -- the name of the claimant or role
    objectDigestInfo  [2] ObjectDigestInfo OPTIONAL
    -- if present, version must be v2
}

ObjectDigestInfo ::= SEQUENCE {
    digestedObjectType ENUMERATED {
        publicKey          (0),
        publicKeyCert      (1),
        otherObjectTypes   (2) },
    -- otherObjectTypes MUST NOT
    -- be used in this profile
    otherObjectTypeID    OBJECT IDENTIFIER OPTIONAL,
    digestAlgorithm       AlgorithmIdentifier,
    objectDigest          BIT STRING
}

```

FIG. 5B
(PRIOR ART)

09734810-051001

Method and system for managing a distributed trust path lookup for public key certificates
relating to the trust path of an X.509 attribute certificate

6/7

AttCertIssuer ::= CHOICE {
 v1Form GeneralNames, -- v1 or v2
 v2Form [0] V2Form -- v2 only
}

V2Form ::= SEQUENCE {
 issuerName GeneralNames OPTIONAL,
 baseCertificateID [0] IssuerSerial OPTIONAL,
 objectDigestInfo [1] ObjectDigestInfo OPTIONAL
 -- at least one of issuerName, baseCertificateID
 -- or objectDigestInfo MUST be present}

IssuerSerial ::= SEQUENCE {
 issuer GeneralNames,
 serial CertificateSerialNumber,
 issuerUID UniqueIdentifier OPTIONAL
}

AttCertValidityPeriod ::= SEQUENCE {
 notBeforeTime GeneralizedTime,
 notAfterTime GeneralizedTime
}

Attribute ::= SEQUENCE {
 type AttributeType,
 values SET OF AttributeValue
 -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

FIG. 5C
(PRIOR ART)

PKClocator ::= SEQUENCE {
 holderPKClocator [0] GeneralNames OPTIONAL,
 authorityPKClocator [1] GeneralNames OPTIONAL
}

wherein GeneralNames is defined by IETF RFC2459 as

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
 otherName [0] OtherName;
 rfc822Name [1] IA5String,
 dNSName [2] IA5String,
 x400Address [3] ORAddress,
 directoryName [4] Name,
 ediPartyName [5] EDIPartyName,
 uniformResourceIdentifier [6] IA5String,
 iPAddress [7] OCTET STRING,
 registeredID [8] OBJECT IDENTIFIER
}

FIG. 6

09734810-051001

Method and system for managing a distributed trust path locator for public key certificates
relating to the trust path of an X.509 attribute certificate

7/7

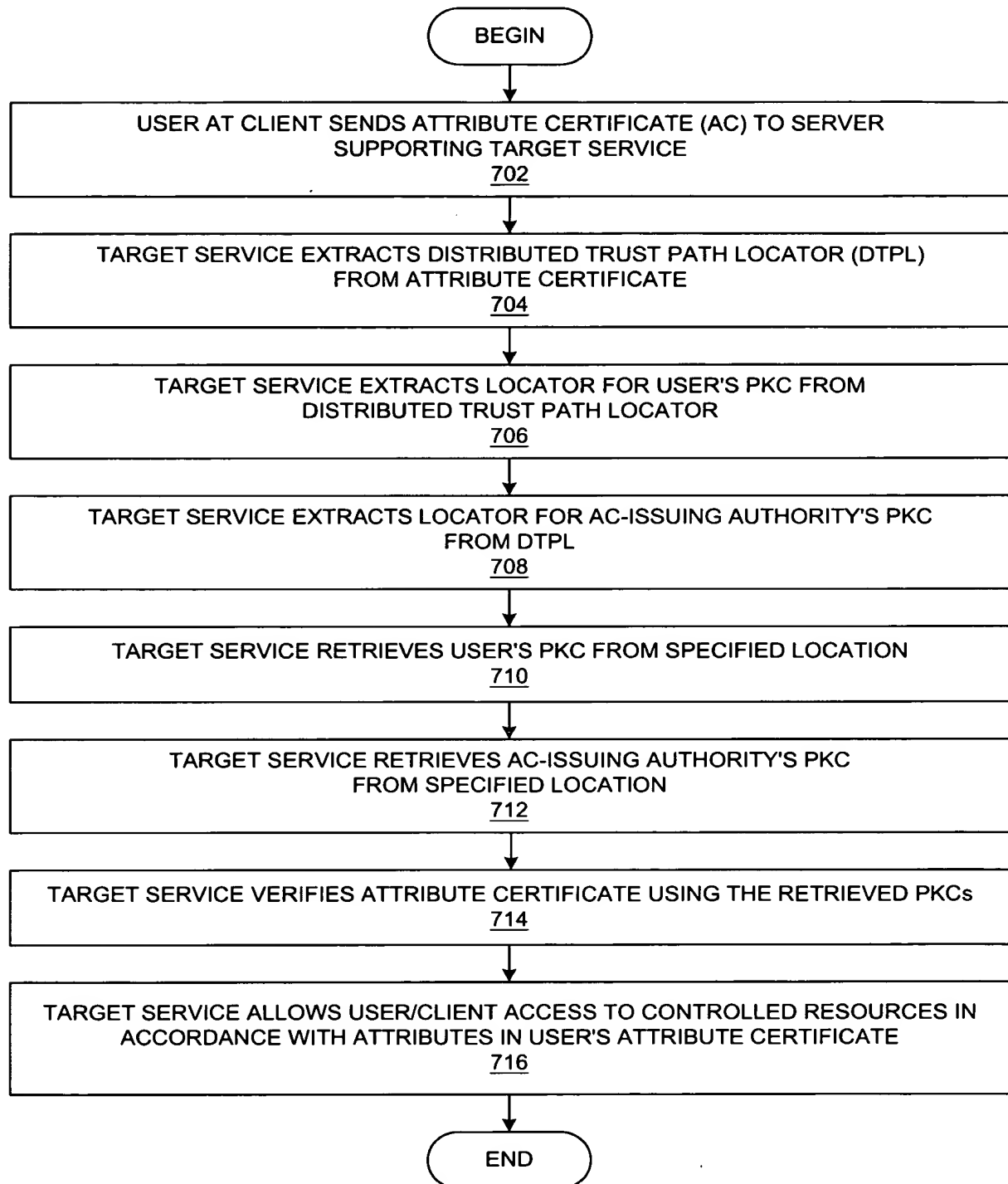


FIG. 7